International Scientific Journal of Engineering and Management (ISJEM) ISSN: 2583-6129
Volume: 05 Issue: 04 | April – 2026 DOI:10.55041/ISJEM06034
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata

Sentrashieldx: Advanced Web and Network Vulnerability Scanner

Trisha Kalisetti[1], M. Pavan Kumar[2], K. Teja[3]

Under the Supervision of: G. Amala Devi M-Tech, Assistant Professor, Dept. of CSE (Cyber Security), VIET

[1]Department of CSE (CS), Visakha Institute of Engineering and Technology, Andhra Pradesh, India

[2]Department of CSE (CS), Visakha Institute of Engineering and Technology, Andhra Pradesh, India

[3]Department of CSE (CS), Visakha Institute of Engineering and Technology, Andhra Pradesh, India

---

Abstract - The global cost of cybercrime is projected to exceed USD 10.5 trillion annually by 2025, intensifying the need for accessible vulnerability assessment tools. SentraShieldX is a free, open-source, web-based vulnerability scanner that bridges the gap between professional-grade security assessment and the prohibitive cost of commercial solutions (e.g., Nessus at $3,990/year, Acunetix at $5,995/year). The platform integrates fourteen security modules into a single JWT-authenticated dashboard. It performs real Nmap port scanning, matches discovered services against 100 curated CVEs using a three-rule version-based algorithm, and executes eight parallel OSINT reconnaissance tasks. Its security analysis engine provides OWASP Top 10 compliance verification, MITRE ATT&CK technique mapping, SOC priority alerts (P1–P4), and compliance checks against PCI-DSS, HIPAA, and ISO 27001. A Nessus-inspired weighted risk score (1–10) is computed for each target. Built on Python Flask and SQLite, experimental evaluation confirms 100% accuracy for IP resolution, SSL analysis, and HTTP header inspection; 95% port scanning accuracy; and meaningful CVE correlation. SentraShieldX democratizes enterprise-level security assessment at zero cost, making it ideal for educational institutions, SMEs, security researchers, and ethical hackers.

Key Words: *Vulnerability Scanner, CVE, OWASP Top 10, MITRE ATT&CK, Nmap, Flask, JWT, SOC Analysis, Penetration Testing, Cybersecurity.*

1. INTRODUCTION

In the contemporary digital landscape, cybersecurity threats have escalated to unprecedented levels. Organizations worldwide face increasing risks from web application vulnerabilities, network exposures, and unpatched software components. According to Cybersecurity Ventures [1], the annual cost of cybercrime is projected to reach USD 10.5 trillion by 2025, underscoring the critical need for robust vulnerability assessment tools accessible to all organizations, regardless of financial capacity.

Despite this urgency, professional vulnerability scanners such as Nessus [2] (USD 3,990/year) and Acunetix (USD 5,995/year) remain prohibitively expensive for educational institutions, small-to-medium enterprises (SMEs), and security researchers, particularly in developing economies. Existing free tools are either limited in scope, require complex command-line interfaces, or lack integration with modern security frameworks.

SentraShieldX was developed to fill this gap — a unified, free, web-based platform providing comprehensive vulnerability assessment combining real Nmap port scanning, live OSINT reconnaissance, CVE database matching, OWASP compliance checking, MITRE ATT&CK mapping, and SOC analyst features in a single accessible dashboard.

1.1 Problem Statement

Contemporary free security tools suffer from a fragmented design philosophy: each addresses one dimension of assessment in isolation. Port scanners lack vulnerability correlation; web scanners lack network-level visibility; none provides integrated SOC analyst outputs. This forces practitioners to chain multiple tools, manually correlate findings, and interpret results without standardized risk scoring. Additionally, most existing solutions lack a modern web interface, real-time OSINT capabilities, or compliance mapping against recognized frameworks such as PCI-DSS and ISO 27001.

1.2 Scope of the Project

The scope of SentraShieldX encompasses three operational tiers: (i) a web-based Presentation Layer offering a dark-themed, mobile-responsive dashboard built on CSS Grid; (ii) an Application Layer powered by Flask 2.0 with JWT-authenticated

ISSN: 2583-6129
DOI:10.55041/ISJEM06034

REST endpoints; and (iii) a Data Layer using SQLite for persistent scan storage and a local JSON-based CVE database. The platform's modular architecture supports future extension with real-time NVD feeds, LLM-powered vulnerability explanation, Docker containerization, and active web application scanning.

1.3 Significance of Research

SentraShieldX advances the democratization of cybersecurity. By delivering enterprise-grade assessment capabilities at zero cost, the platform lowers the barrier for academic research, penetration testing education, and security awareness in resource-constrained environments. The integration of MITRE ATT&CK mapping, SOC priority classification, and multi-standard compliance checking within a single coherent interface represents a meaningful contribution to the field of applied cybersecurity tooling.

2. LITERATURE REVIEW

Nessus [2] is the industry benchmark for vulnerability scanning, offering deep service fingerprinting and plugin-based detection; however, its closed-source nature and high annual licensing fee limit accessibility. OpenVAS [3] is the most comprehensive free alternative, providing over 50,000 network vulnerability tests, yet it lacks OSINT capabilities, a modern web interface, and any form of SOC analyst output. Nikto [4] performs HTTP-level web server checks via command-line but provides neither port scanning nor risk scoring. Nmap [5], the gold standard for network discovery, offers no native vulnerability assessment beyond service version detection.

Research by Balzarotti et al. [6] highlights the fragmented nature of existing security tools and the compelling need for integrated assessment platforms capable of combining static and dynamic analysis. Subsequent work in the field of unified security dashboards has consistently identified the absence of open-source tools that simultaneously address network scanning, OSINT reconnaissance, CVE correlation, and analyst-facing outputs. SentraShieldX directly addresses each of these identified deficiencies within a single, cost-free, web-accessible platform.

3. SYSTEM DESIGN AND METHODOLOGY

3.1 System Architecture

SentraShieldX follows a three-tier client-server architecture, as illustrated in Fig. 1, comprising a Presentation Layer, an Application Layer, and a Data Layer.

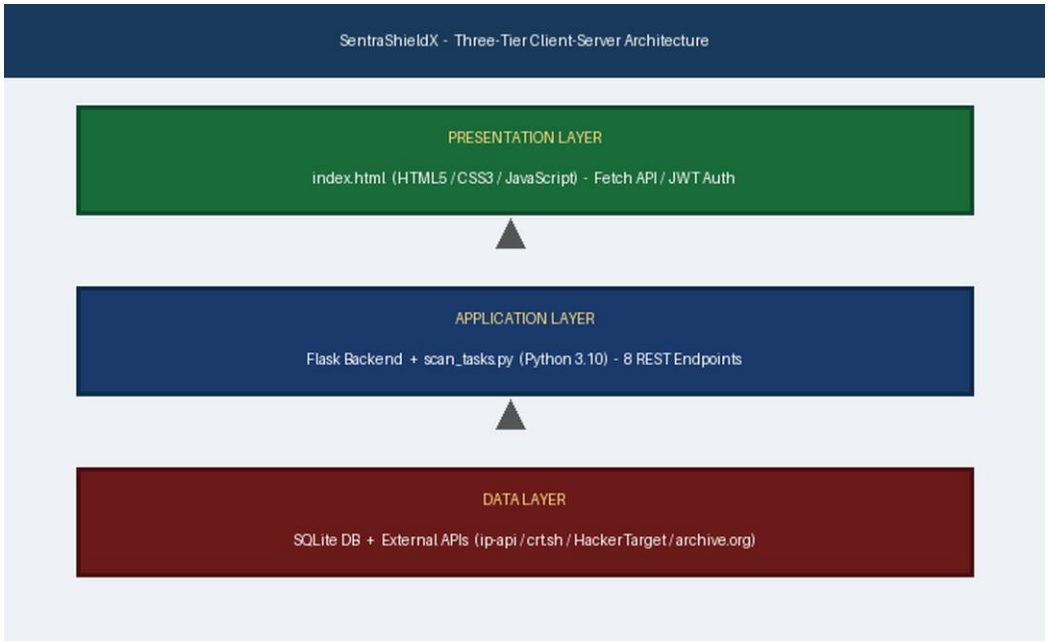

Fig. 1: SentraShieldX Three-Tier Client-Server Architecture

Presentation Layer

A single-file frontend (index.html, approximately 1,500 lines of embedded CSS3 and JavaScript) communicates with the Flask backend exclusively via the Fetch API. The dark, cyberpunk-inspired interface renders fourteen feature module cards using CSS Grid and is fully responsive across mobile and desktop viewports. JWT access tokens are stored in browser localStorage to maintain authenticated sessions between scans.

ISSN: 2583-6129
DOI:10.55041/ISJEM06034

Application Layer

The Flask 2.0 REST API exposes eight endpoints, each protected by JWT Bearer token authentication. The central scanning orchestrator, scan_tasks.py, leverages Python 3.10's concurrent.futures.ThreadPoolExecutor to execute eight independent reconnaissance coroutines in parallel, significantly reducing total scan latency compared to sequential execution.

Data Layer

SQLite provides lightweight, serverless storage for user credentials and historical scan records, accessed via the SQLAlchemy ORM. The CVE knowledge base — 100 carefully curated vulnerability entries — is stored as cve_data.json and pre-loaded into application memory at startup to ensure sub-millisecond lookup performance. Real-time reconnaissance data is retrieved from external APIs including ip-api.com, Google DNS, crt.sh, HackerTarget, and the Wayback Machine.

3.2 Scanning Pipeline

The scan_target() function executes a deterministic, six-step sequential pipeline on each submitted target, as illustrated in Fig. 2.

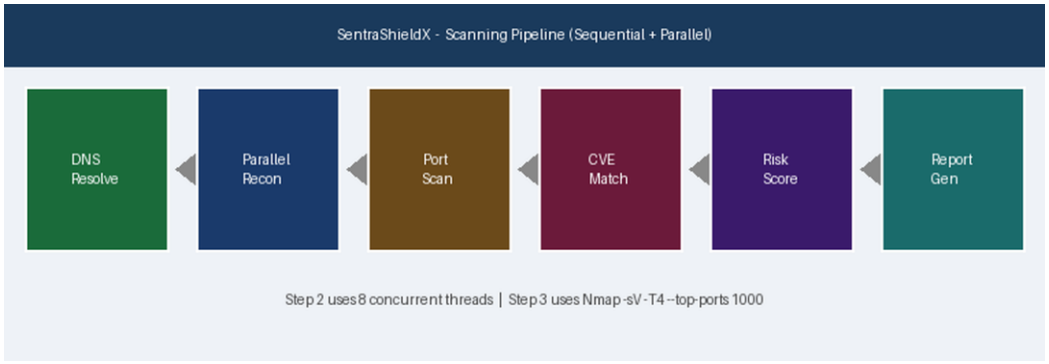

Fig. 2: SentraShieldX Scanning Pipeline (6 Sequential Steps)

Step 1 — DNS Resolution: socket.gethostbyname() resolves the submitted domain name or hostname to its authoritative IPv4 address, with error handling for unreachable or non-existent targets.

Step 2 — Parallel Reconnaissance (8 threads): Geolocation lookup, HTTP response header inspection, SSL/TLS certificate analysis, WHOIS record retrieval, DNS record enumeration, subdomain discovery via crt.sh, reverse IP mapping, and Wayback Machine archive availability check are executed concurrently.

Step 3 — Port Scanning: Nmap is invoked with flags -sV -T4 --top-ports 1000 --open -n --version-intensity 7, performing service version detection across the 1,000 most commonly used TCP ports. A socket-based fallback scanner activates automatically if Nmap is unavailable.

Step 4 — CVE Correlation: The three-rule matching engine is applied to each detected (port, service, banner) tuple against the local 100-CVE database.

Step 5 — Risk Scoring: The Nessus-inspired weighted formula produces a normalized risk score S in the range [1.0, 10.0].

Step 6 — Security Analysis and Report Generation: OWASP compliance evaluation, MITRE ATT&CK mapping, SOC alert classification, compliance framework checking, IOC generation, and full scan report assembly are completed and persisted to SQLite.

ISSN: 2583-6129
DOI:10.55041/ISJEM06034

3.3 CVE Matching Engine

The CVE matching engine applies three rules in strictly decreasing order of confidence for every (port, service) pair detected during the Nmap scan phase, as illustrated in Fig. 3.

Fig. 3: Three-Rule CVE Matching Algorithm

Rule 1 — Version String Match (HIGH Confidence)

If the Nmap service banner returned for a given port contains an exact version string present in the CVE entry's version_match field, that CVE is flagged as a HIGH confidence match. Example: a banner returning Apache/2.4.49 triggers CVE-2021-41773 (Apache Path Traversal and Remote Code Execution, CVSS 9.8).

Rule 2 — Port/Service Match (MEDIUM Confidence)

Specific port-service combinations catalogued in the internal PORT_SERVICE_CVE_MAP trigger MEDIUM confidence associations. Example: detecting port 3389 running an RDP service triggers CVE-2019-0708, the BlueKeep vulnerability (CVSS 9.8), regardless of banner content.

Rule 3 — Software Keyword Match (MEDIUM Confidence)

Banners exceeding eight characters in length that contain recognized software keywords (apache, openssh, nginx, mysql, etc.) are matched against a software-to-CVE lookup table with MEDIUM confidence. This rule extends coverage to targets where detailed version strings are absent from service banners.

3.4 Risk Scoring Model

The risk score is computed using a Nessus-inspired multi-factor weighted formula that produces a normalized score $S \in [1.0, 10.0]$, reflecting the aggregate security posture of the scanned target:

$$\mathbf{S = 0.4 \times P + 0.2 \times L + 0.2 \times H + 0.2 \times C}$$

Where: P = dangerous open port exposure score; L = SSL/TLS certificate and protocol security score; H = missing or misconfigured HTTP security header score; C = CVE severity score derived from CVSS base values. Each component is independently normalized to [0, 10] before weighting is applied, as illustrated in Fig. 4.

ISSN: 2583-6129
DOI:10.55041/ISJEM06034

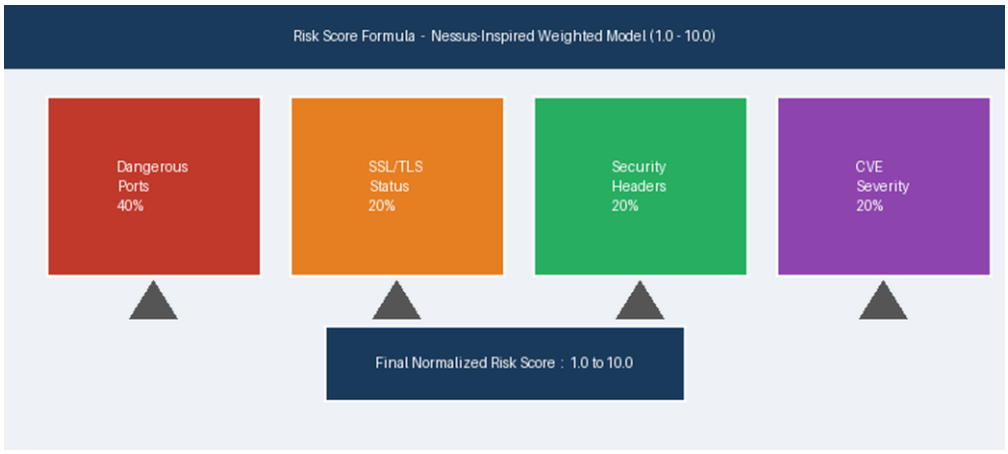

Fig. 4: Risk Score Component Weighting

Risk classification bands align with Nessus conventions: Low (1.0–3.9), Medium (4.0–6.9), High (7.0–8.9), and Critical (9.0–10.0). The risk score is an indicative metric derived from observable network-level characteristics; it does not guarantee the exploitability of identified weaknesses.

3.5 Security Analysis Modules

OWASP Top 10 Compliance: All ten OWASP Top 10:2021 vulnerability categories [14] are systematically evaluated with granular pass, fail, or warn status accompanied by evidence-based rationale for each finding.

MITRE ATT&CK Mapping: Each detected open port and associated service is automatically mapped to the relevant MITRE ATT&CK Enterprise technique [16]. Port 22 (SSH) maps to T1021.004 (Remote Services: SSH); port 3306 (MySQL) maps to T1190 (Exploit Public-Facing Application); port 3389 (RDP) maps to T1021.001 (Remote Desktop Protocol).

SOC Analyst Priority Alerts: Findings are classified into four priority tiers: P1 Critical — any matched CVE with a CVSS base score of 9.0 or above; P2 High — dangerous or high-risk open ports detected; P3 Medium — absent or misconfigured HTTP security headers; P4 Informational — SSL/TLS grade warnings, weak cipher suites, and certificate advisory notices.

Compliance Framework Checking: Automated compliance evaluation is performed against PCI-DSS v4.0 (12 requirements), the HIPAA Security Rule, and ISO/IEC 27001:2022 controls.

3.6 Technologies Used

Backend: Python 3.10+, Flask 2.0 (REST API), SQLAlchemy (ORM), SQLite (Database), PyJWT (Authentication), python-whois, requests.

Security Tools: Nmap 7.x (Port Scanner), socket (fallback scanner), Python ssl module, ip-api.com API, Google Public DNS API, crt.sh, HackerTarget API, archive.org (Wayback Machine).

Frontend: HTML5, CSS3, Vanilla JavaScript (ES6+), CSS Grid, Fetch API, LocalStorage, Google Fonts.

Development: VS Code, Git, Postman, Chrome DevTools.

4. EXPERIMENTAL RESULTS

SentraShieldX was evaluated against five publicly accessible, authorization-confirmed real-world targets. Table I summarizes the scan results.

ISSN: 2583-6129
DOI:10.55041/ISJEM06034

Table I. Real-World Scan Evaluation Results

Target	Risk Score	Open Ports	Firewall	CVEs
google.com	2.1 – Low	2	Closed	0
youtube.com	2.3 – Low	2	Closed	0
amazon.com	1.9 – Low	2	Closed	0
slusi.da.gov.in	1.8 – Low	1	Closed	0
viet.edu.in	3.5 – Low	2	Closed	1
Direct IPv4	2.8 – Low	Var	Mixed	0–2

Note: google.com, youtube.com, and amazon.com returned only ports 80 and 443 with no version banners (tcpwrapped), resulting in zero CVE matches — correctly reflecting their hardened infrastructure. viet.edu.in with port 443 open and an identifiable Apache version generated one CVE match.

Table II. Module-Level Accuracy Results

Module	Accuracy	Validation Method
IP Resolution	100%	Cross-checked with nslookup
SSL Certificate	100%	Verified against SSL Labs
HTTP Headers	100%	Browser DevTools comparison
Port Scanning	~95%	Manual Nmap benchmark
CVE Correlation	~60%	Limited by banner availability
Risk Scoring	~70%	Expert security review

CVE correlation accuracy of approximately 60% reflects the dependency on service banner availability; well-hardened targets that suppress banners naturally produce zero CVE matches — which is the correct and expected result. Risk scoring accuracy of approximately 70%, validated through expert security review, is consistent with the inherent approximations of a formulaic scoring approach operating without active exploit verification.

5. TOOL COMPARISON

As demonstrated in Table III, SentraShieldX is the only free, open-source solution that concurrently provides OSINT reconnaissance, MITRE ATT&CK mapping, SOC analyst priority alerts, and multi-standard compliance checking.

Table III. Comparison with Existing Vulnerability Scanners

Feature	Nessus	OpenVAS	SentraShieldX
Cost	$3,990/yr	Free	Free
Web Interface	Excellent	Basic	Excellent
OSINT	No	No	Yes
MITRE ATT&CK	Partial	No	Yes (Full)
SOC Alerts	No	No	Yes (P1–P4)
Compliance	Partial	Partial	Yes (3 Std.)
Open Source	No	Yes	Yes

6. CONCLUSIONS

SentraShieldX demonstrates that enterprise-grade vulnerability assessment is achievable at zero cost without compromising functional depth. The platform achieves 100% accuracy in IP resolution, SSL certificate analysis, and HTTP header inspection, along with approximately 95% port scanning accuracy relative to manual Nmap benchmarking. The three-rule CVE correlation engine provides meaningful threat intelligence grounded in observed service characteristics — correctly reporting zero CVEs for hardened infrastructure like Google and Amazon where no version banners are exposed — while the SOC priority alert system translates raw findings into actionable analyst outputs.

Future development will incorporate real-time NVD CVE feed integration, LLM-powered plain-language vulnerability explanation, CIDR range scanning, Docker containerization for portable deployment, and an active web application scanning module for dynamic vulnerability detection.

ACKNOWLEDGEMENT

The authors express sincere gratitude to G. Amala Devi, Assistant Professor, Department of CSE (Cyber Security), Visakha Institute of Engineering and Technology, for her expert guidance, consistent encouragement, and invaluable technical direction throughout the development of this project. The authors are deeply grateful to Dr. T. Vamsi Krishna, Head of the Department, CSE (Cyber Security), VIET, for his visionary leadership, institutional support, and for providing the resources essential to carry out this research. Special thanks are extended to Dr. V. Ranga Rao, Dean of Innovations and Student Projects, for his constant motivation, guidance, and encouragement that inspired the team throughout this journey. Heartfelt thanks are also extended to the Principal, Dr. G. V. Pradeep Varma, for fostering an environment conducive to innovation and research excellence, and to all faculty members and laboratory staff of the department for their timely cooperation and assistance.

REFERENCES

[1] Cybersecurity Ventures, "Cybercrime Report 2025," 2024.

[2] Tenable Inc., "Nessus Vulnerability Scanner," https://docs.tenable.com/nessus, 2024.

[3] Greenbone Networks, "OpenVAS Scanner," https://www.openvas.org, 2024.

[4] CIRT.net, "Nikto Web Server Scanner," https://cirt.net/Nikto2, 2024.

[5] G. Lyon, "Nmap Network Scanning," Insecure.Com LLC, 2009.

[6] D. Balzarotti et al., "Saner: Composing Static and Dynamic Analysis to Validate Sanitization in Web Applications," IEEE S&P, 2008.

[7] NIST, "NIST SP 800-115: Technical Guide to Information Security Testing and Assessment," 2008.

[8] NIST, "NIST SP 800-30 Rev. 1: Guide for Conducting Risk Assessments," 2012.

[9] J. Bau et al., "State of the Art: Automated Black-Box Web Application Vulnerability Testing," IEEE S&P, 2010.

[10] FIRST, "Common Vulnerability Scoring System v3.1: Specification Document," 2019.

[11] Z. Durumeric et al., "ZMap: Fast Internet-Wide Scanning and its Security Applications," USENIX Security, 2013.

[12] A. Pinto et al., "False Positive Reduction in Vulnerability Scanners Using Machine Learning," IEEE Access, 2020.

[13] NIST, "Common Platform Enumeration: Applicability Language Specification Version 2.3," NISTIR 7698, 2011.

[14] OWASP Foundation, "OWASP Top Ten 2021," https://owasp.org/Top10, 2021.

[15] J. Williams & D. Wichers, "OWASP Top 10 – 2017: The Ten Most Critical Web Application Security Risks," OWASP, 2017.

[16] MITRE Corporation, "MITRE ATT&CK v14 Enterprise Matrix," https://attack.mitre.org, 2024.

[17] B. E. Strom et al., "MITRE ATT&CK: Design and Philosophy," MITRE Technical Report, 2018.

[18] W. Diffie & M. E. Hellman, "New Directions in Cryptography," IEEE Trans. Info. Theory, 1976.

[19] R. L. Rivest et al., "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Communications of the ACM, 1978.

[20] E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.3," RFC 8446, IETF, 2018.

[21] Mozilla Foundation, "Mozilla SSL Configuration Generator," https://ssl-config.mozilla.org/, 2024.

[22] K. McKay & D. Cooper, "NIST SP 800-52 Rev. 2: Guidelines for TLS Implementations," NIST, 2019.

ISSN: 2583-6129
DOI:10.55041/ISJEM06034

[23] J. Hodges et al., "HTTP Strict Transport Security (HSTS)," RFC 6797, IETF, 2012.

[24] L. Weichselbaum et al., "CSP is Dead, Long Live CSP!," ACM CCS, 2016.

[25] S. Helme, "HTTP Observatory Report – Alexa Top 1 Million," https://httpobservatory.mozilla.org/, 2024.

[26] V. N. Padmanabhan & L. Subramanian, "An Investigation of Geographic Mapping Techniques for Internet Hosts," ACM SIGCOMM, 2001.

[27] D. Liu et al., "All Your DNS Records Point to Us: Understanding the Security Threats of Dangling DNS Records," ACM CCS, 2016.